Axborotni himoyalashda tarmoqlararo ekranlarning o’rni

Reja:

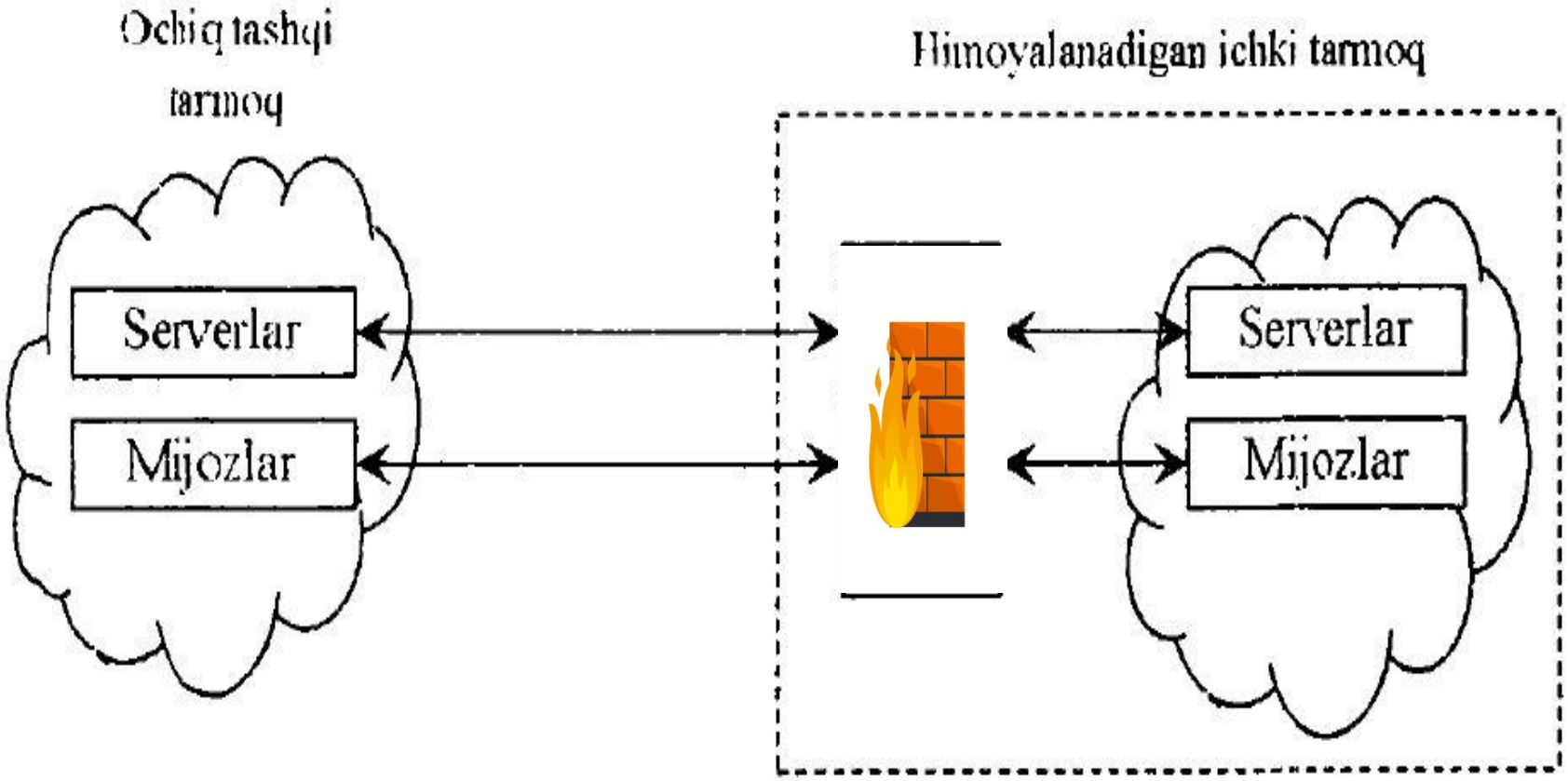
1. **Tarmoqlararo ekranlarning ishlash xususiyatlari**
2. **Tarmoqlararoekranlarning asosiy komponentlari**
3. **Tarmoqlararo ekranlar asosidagi tarmoq himoyasining sxemalari**

Tarmoqlararo ekranlaming ishlash xususiyatlari

- Tarmoqlararo ekran (TE) - *Brandmauer* yoki *firewall sistemasi* deb ham ataluvchi tarmoqlararo himoyaning ixtisoslashtirilgan kompleksi. Tarmoqlararo ekran umumiy tarmoqni ikki yoki undan ko‘p qismlarga ajratish va ma’lum paketlarini chegara orqali umumiy tarmoqning bir qismidan ikkinchisiga o'tish shartlarini belgilovchi qoidalar to‘plamini amalga oshirish imkonini beradi.

Tarmoqlararo ekran quyidagi ikkita vazifani bajarishi kerak:

- - tashqi (himoyalanuvchi tarmoqqa nisbatan) foydalanuvchilarning korporativ tarmoqning ichki resurslaridan foydalanishini chegaralash.
- Bunday foydalanuvchilar qatoriga tarmoqlararo ekran himoyalovchi ma’lumotlar bazasining serveridan foydalanishga urinuvchi sheriklar, masofadagi foydalanuvchilar, xakerlar, hatto kompaniyaning xodimlari kiritilishi mumkin;
- - himoyalanuvchi tarmoqdan foydalanuvchilarning tashqi resurslardan foydalanishlarini chegaralash. Bu masalaning yechilishi, masalan, serverdan xizmat vazifalari talab etmaydigan foydalanishni tartibga solishga imkon beradi.



8.1-rasm. Tarmoqlararo ekranni ulash sxemasi.

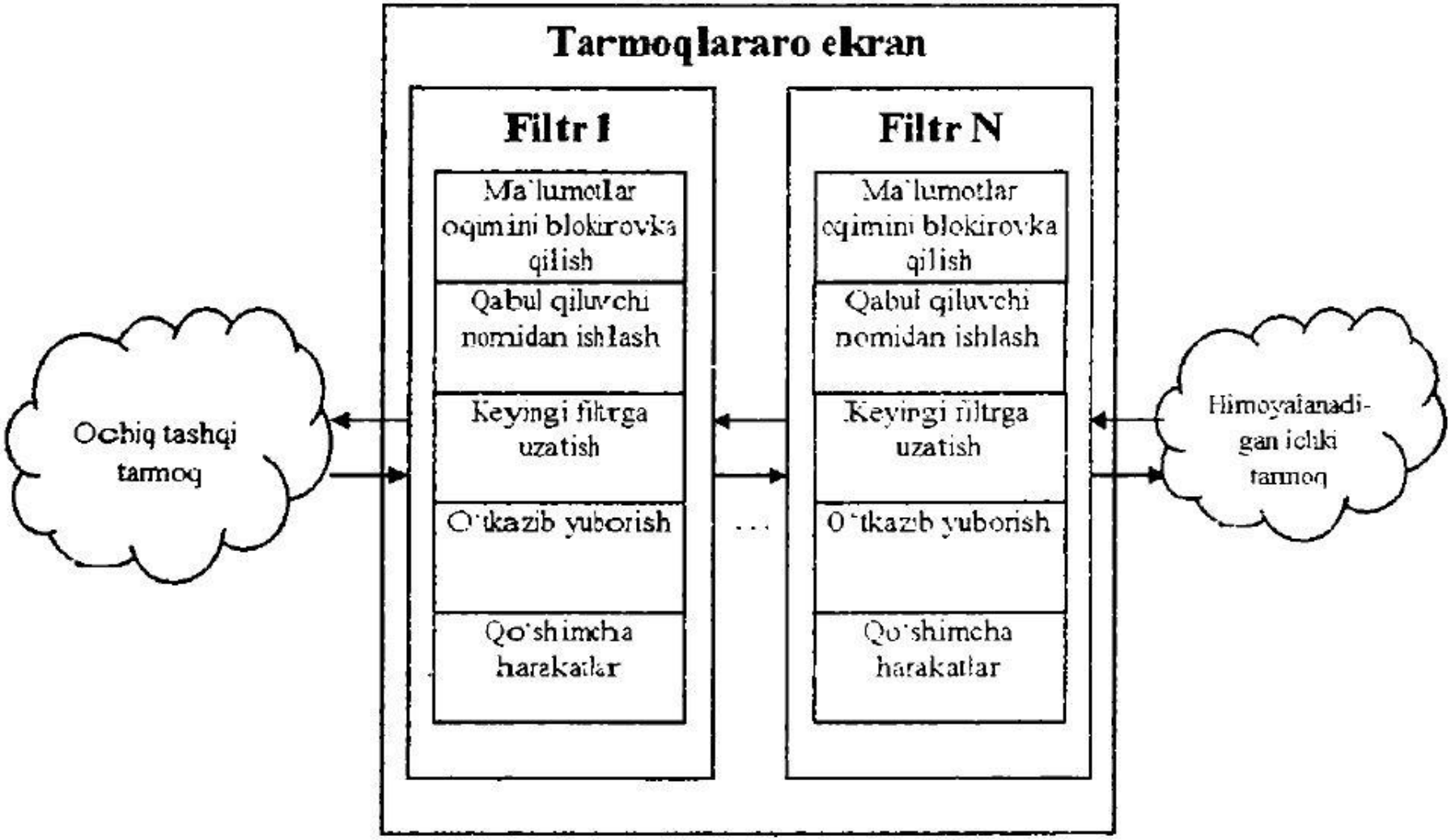
Hozirda ishlab chiqarilayotgan tarmoqlararo ekranlarning tavsiflariga asoslangan holda, ulami quyidagi asosiy alomatlari bo‘yicha turkumlash mumkin:

- *OSI modeli sathlarida ishlashi bo ‘yicha.*
- - paketli filtr (ekranlovchi marshrutizator - screening router);
- - seans sathi shlyuzi (ekranlovchi transport);
- -tatbiqiy sath shlyuzi (application gateway);
- - ekspert sathi shlyuzi (stateful inspection firewall).

- *Ishlatiladigan texnologiya bo 'yicha:*
- - protokol holatini nazoratlash (Stateful inspection);
- - vositachilar modullari asosida (proxy);
- *Bajarilishi bo 'yicha:*
- - apparat-dasturiy;
- - dasturiy;
- *Ulanish sxemasi bo 'yicha;*
- - tarmoqni umumiy himoyalash sxemasi;
- - tarmoq segmentlari himoyalanuvchi berk va tarmoq segmentlari himoyalanmaydigan ochiq sxema;
- - tarmoqning berk va ochiq segmentlarini alohida himoyalovchi
- sxema.

Trafiklarni filtrlash

- *Trafiklarni filtrlash* Axborot oqimlarini filtrlash, ularni ekran orqali, ba’zida qandaydir o‘zgartirishlar bilan o ‘tkazishdan iborat.
- Filtrlash, qabul qilingan xavfsizlik siyosatiga mos keluvchi, ekranga oldindan yuklangan qoidalar asosida amalga oshiriladi. Shu sababli, tarmoqlararo ekranni axborot oqimlarini ishlovchi filtrlar ketmaketligi sifatida tasavvur etish qulay



8.2-rasm. Tarmoqlararo ekran tuzilmasi.

Vositachilik funksiyalar

- *Vositachilik funksiyalarining bajarilishi* Tarmoqlararo ekran vositachilik funksiyalarini *ekranlovchi agentlar* yoki *vositachi dasturlar* deb ataluvchi maxsus dasturlar vordamida bajaradi. Bu dasturlar rezident dasturlar hisoblanadi hamda tashqi va ichki tarmoq orasida xabarlar paketini bevosita uzatishni taqiqlaydi.

Umuman, vositachi-dasturlar, xabarlar oqimini shaffof uzatilishini blokirovka qilgan holda, quyidagi funksiyalarni bajarishi mumkin:

- **- uzatiluvchi va qabul qilinuvchi ma’lumotlarning haqiqiyligini tekshirish;**
- **- ichki tarmoq resurslaridan foydalanishni chegaralash;**
- **- tashqi tarmoq resurslaridan foydalanishni chegaralash;**
- **- tashqi tarmoq dan so‘raluvchi ma’lumotlami kesh xotiraga saqlash;**

- **- xabarlar oqimini filtrlash va o ‘zgartirish, masalan, viruslarni dinamik tarzda qidirish va axborotni shaffof shifrlash;**
- **- foydalanuvchilarni identifxkatsiyalash va autentifikatsiyalash;**
- **- ichki tarmoq adreslarini translyatsiyalash;**
- **- hodisalami qaydlash, hodisalarga reaksiya ko‘rsatish hamda qaydlangan axborotni tahlillash va hisobotlami generatsiyalash.**

Uzatiluvchi va qabul qilinuvchi ma ’lumotlaming haqiqiyligini tekshirish

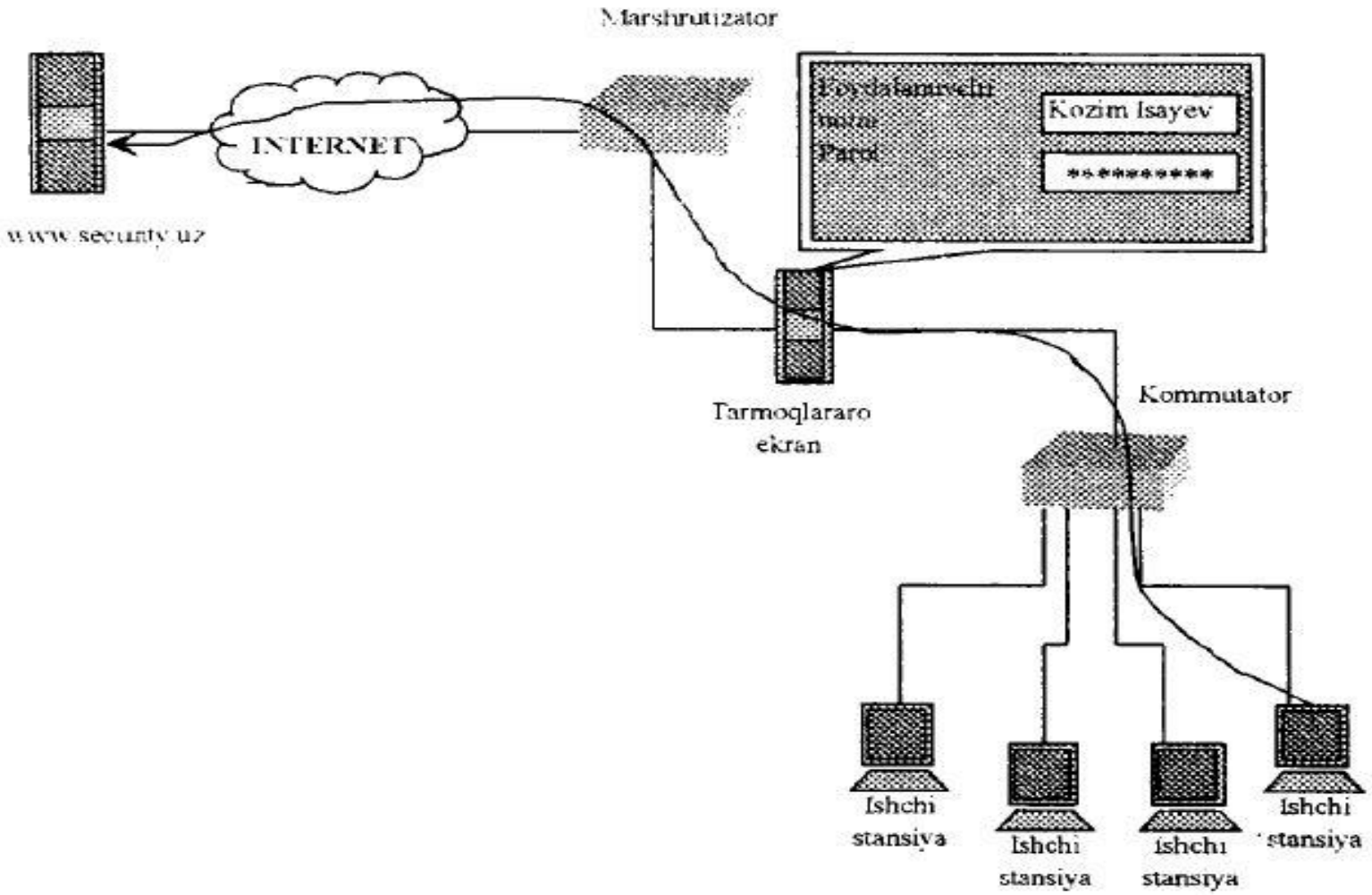
- nafaqat elektron xabarlarni, balki soxtalashtirilishi mumkin boigan migratsiyalanuvchi dasturlarni (Java, ActiveXControls) autentifkatsivalash uchun dolzarb hisoblanadi. Xabar va dasturlarning haqiqiyligini tekshirish ulaming raqamli imzosmi tekshirishdan iboratdir.

- *Ichki tarmoq resurslaridan foydalanishni chegaralash* usullari operatsion tizim sathida madadlanuvchi chegaralash usullaridan farq qilmaydi.
- *Tashqi tarmoq resurslaridan foydalanishni chegarlashda* ko‘pincha quyidagi yondashishlardan biri ishlatiladi:
- - faqat tashqi tarmoqdagi berilgan adres bo‘yicha f'oydalanishga ruxsat berish;
- - yangilanuvchi nojoiz adreslar ro‘yxati bo‘yicha so'rovlarni filtrlash va o ‘rinsiz kalit so'zlari bo‘yicha axborot resurslarini qidirishni blokirovka qilish:

- *ma’lumotlami keshlash* maxsus vositachilar yordamida madadlanadi. Ichki tarmoq foydalanuvchilari tashqi tarmoq resurslaridan foydalanganlarida barcha axborot,
- proxy-server deb ataluvchi brandmauer qattiq diski makonida to‘planadi.

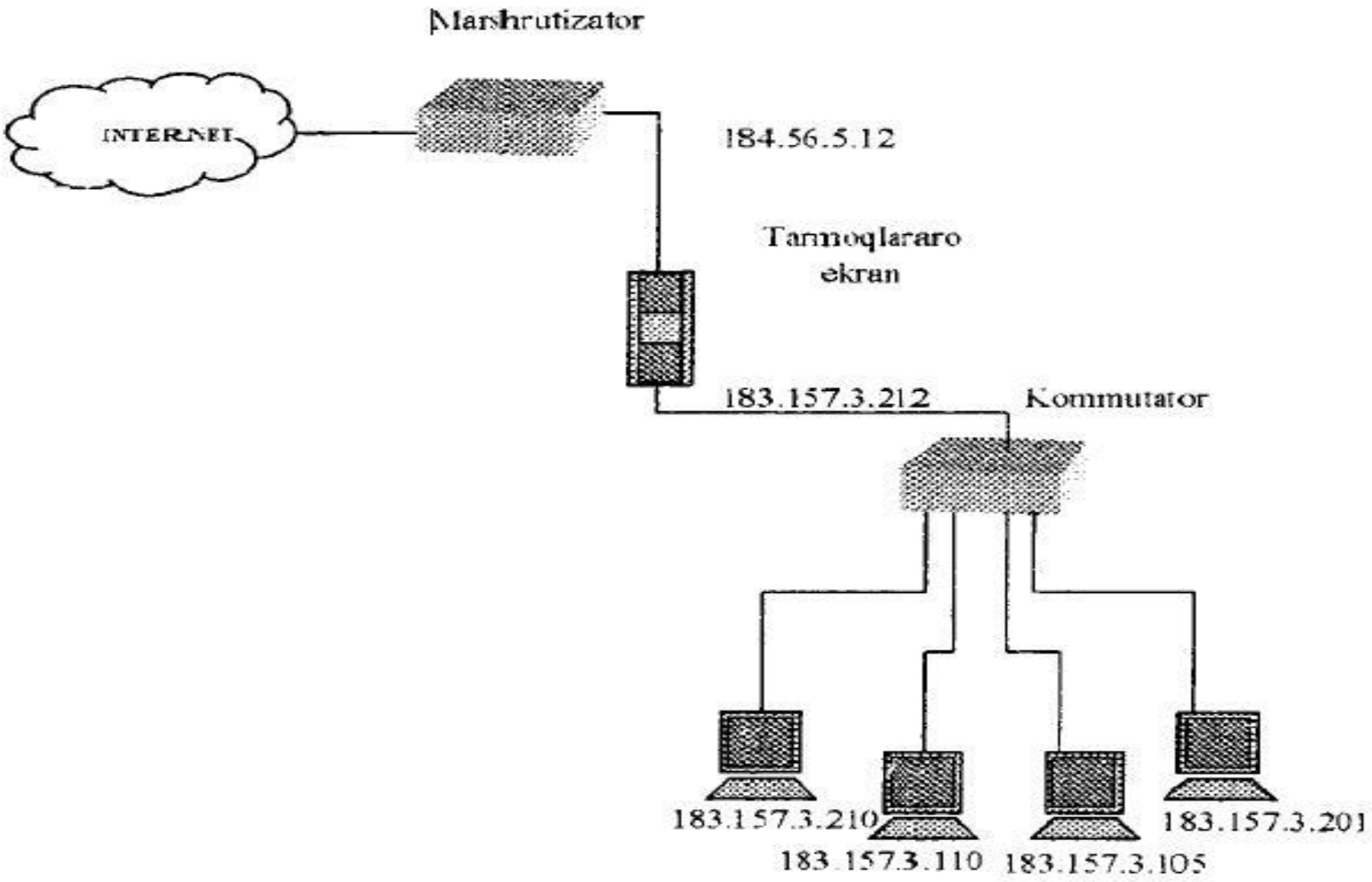
- *Xabarlar oqimini filtrlash va o'zgartirish* vositachi tomonidan
- qoidalarning berilgan to‘plami yordamida bajariladi. Bunda vositachi- dasturlarning ikki xili farqlanadi:
- - servis turini aniqlash uchun xabarlar oqimini tahlillashga mo‘ljallangan ekranlovchi agentlar, masalan, FTP, HTTP, Telnet;
- - barcha xabarlar oqimini ishlovchi universal ekranlovchi agentlar, masalan, kompyuter viruslarini qidirib zararsizlantirishga yoki ma’lumotlami shaffof shifrlashga mo’ljallangan agentlar.

- *Foydalanuvchilarni identifikatsiyaiash va autentifikatsiyalash*
- ba’zida oddiy identifikatorni (ism) va parolni taqdim etish bilan amalga oshiriladi. Ammo bu sxema xavfsizlik nuqtayi nazaridan zaif hisoblanadi, chunki parolni begona shaxs ushlab qolib, ishlatishi mumkin. Internet tarmog‘idagi ko'pgina mojarolar qisman an’anaviy ko‘p marta ishlatiluvchi parollarning zaifligidan kelib chiqqan.



8.3-rasm. Parol bo‘yicha foydalanuvchini autentifikatsiyalash sxemasi.

- *Ichki tarmoq adreslarini translyatsiyalash.* Ko‘pgina hujumlarni amalga oshirishda niyati buzuq odamga qurbonining adresini bilish kerak bo‘ladi. Bu adreslami hamda butun tarmoq topologiyasini bekitish uchun tarmoqiararo ekranlar eng muhim vazifani – ichki tarmoq adreslarini translyatsiyalashni bajaradi .
- Bu funksiya ichki tarmoqdan tashqi tarmoqqa uzatiluvchi barcha paketlarga nisbatan bajanladi. Bunday paketlar uchun jo ‘natuvchi kompyuterlarning IP-adreslari bitta "ishonchli" IP-adresga avtomatik tarzda o'zgartiriladi.



8.4-rasm. Tarmoq adreslarini translatsiyalash.

- *Hodisalami qaydlash, hodisalarga reaksiya ko'rsatish hamda qaydlangan axborotni tahlillash va hisobodarni generatsiyalash* tarmoqlararo ekranlarning muhim vazifalari hisoblanadi. Korporativ tarmoqni himoyalash tizimining jiddiy elementi sifatida tarmoqlararo ekran barcha harakatlarni ro‘yxatga olish imkoniyatiga ega.